Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

ROUTING AND TRANSMITTAL SLIP 5/23/85

TO: (Name, office symbol, room number, building, Agency/Post)	Initials	Date
1. D/SECURITY		
2.		
3.		
4.		
5.		

Action	File	Note and Return
Approval	For Clearance	Per Conversation
As Requested	For Correction	Prepare Reply
Circulate	For Your Information	See Me
Comment	Investigate	Signature
Coordination	Justify	

REMARKS

#1 - FOR ACTION

(PLS PROVIDE DIRECT RESPONSE WITH DROP CY TO ER AND EO/DDA.)

SUSPENSE: 3 JUNE 85

This is ER suspense date. If it is too short (with May 27 holiday) call us for extension.

STAT

STAT NOT use this form as a RECORD of approvals, concurrences, disposals, clearances, and similar actions

STAT FROM: Room No.—Bldg.

Phone No.

5041-102 OPTIONAL FORM 41 (Rev. 7-76) Prescribed by GSA FPMR (41 CFR) 101-11.206

* GPO: 1983 O - 381-529 (232)

EXECUTIVE SECRETARIAT

ROUTING SLIP

TO:		ACTION	INFO	DATE	INITIAL
1	DCI				
2	DDCI				
3	EXDIR		X		
4	D/ICS				
5	DDI		X		
6	DDA	X			
7	DDO				
8	DDS&T		X		
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/Pers				
14	D/OLL				
15	D/PAO				
16	SA/IA				
17	AO/DCI				
18	C/IPD/OIS				
19					
20					
21					
22					
	SUSPENSE	3 June 1985 Date			

10-1

Remarks

To 6: Please prepare appropriate response and provide ER with an information copy.

Executive Secretary

22 May 1985

Date

3637 (10-81)

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

Executive Registry
85- 2089

Bell Technical Operations TEXTRON

Bell Technical Operations Corporation
Subsidiary of Textron Inc.

1050 East Valencia Road
Tucson, Arizona 85706
602/294-2651
TWX 910-952-1103

DD/A Registry
85-826

May 6, 1985

Director
Central Intelligence Agency
Washington, DC 20505

Dear Sir:

Bell Technical Operations Textron has been asked by Sandia National Laboratories to conduct a number of tasks related to the evaluation and upgrading of communications. One of these tasks is to produce an analysis of the electromagnetic threat to sensitive Department of Energy (DOE) facilities supported by Sandia. This analysis is directed at the terrorist threat, as defined in the attached, and will be focused primarily on the communications used by security forces at these facilities.

In order to conduct this analysis, it is essential that information on known, suspected, potential exploitation or degradation of electronic systems by terrorists and other illicit organizations be collected. Enclosure 1 is a list of the types of threat information that is needed for the analysis. To facilitate your response, a brief questionnaire and a return envelope have been provided at enclosure 2. It is requested that you complete and return the questionnaire. Negative replies are also requested.

Should you have information on the subject that can be made available for this analysis, a representative will contact your point of contact and make the necessary arrangements for obtaining or reviewing the material.

The following is provided should you desire additional information from us:

Bell Technical Operations Corporation
1050 E. Valencia Road
Tucson, Arizona 85706
(602) 294-2651
Points of contact:
Mr. Gerald Cody (ext. 239)
Mr. David Bunker (ext. 223)

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

Bell Technical Operations has a DOD Top Secret facility clearance (FSC 7B147). The cognizant security office is:

Defense Investigative Service
Southwestern Region
1136 Washington Avenue
St. Louis, Missouri 63101
(314) 263-6581

Should you desire to establish a further need-to-know on Bell's part, the following information is provided:

Sandia National Laboratories
Contract Nr. 59-8778
Dated 11 April, 1985
"Security Communications Research and Development"
Sandia POC: Mr. David J. Gangel
(505) 844-4206

Any assistance or information that you can provide us in accomplishing this critical task, will be greatly appreciated.

Very respectfully,

David L. Bunker
Project Manager

/dw

encls: a/s

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

10. To what extent do terrorists use radio communications equipment/systems? Are communications encrypted/coded?

11. Are there any terrorist plans, documents, or other items that refer to or indicate the possibility of any of the above questions happening? If so, by whom, when, where, and to what extent?

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

SUBJECT: TERRORIST THREAT ANALYSIS

From:

1. ☐ We have information that relates to your task and can assist in answering questions _____ on enclosure one.

2. ☐ We have additional information available that can assist you.

3. ☐ The information we have is classified up to _____.

4. ☐ We have no information that can assist you.

5. ☐ We have information, but it is not releasable because:

_____

_____

_____

6. ☐ We will attempt to assist you in your efforts. Please contact:

_____

_____

_____

_____

Enclosure 2

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

Armed Forces Communications
and Electronics Association
AFCEA International Headquarters Building
5641 Burke Centre Parkway • Burke, VA 22015
Telephone (703) 425-8500 • Telex 90 1114 AFCEA BURK

85-1851

Executive Registry
85-
1393/1

May 16, 1985

William J. Casey
Director
Central Intelligence Agency
Washington, D.C. 20505

Dear Mr. Casey:

Enclosed is a copy of the May 1985 issue of **SIGNAL Magazine** which contains your article **"Protecting Our Secrets: Renewing the Commitment."**

It was privilege for the Armed Forces Communications and Electronics Association and for me personally to have featured your article in the May 1985 issue of SIGNAL. I know that the readers of SIGNAL will find your remarks very interesting.

Sincerely,

Jon L. Boyes

Dr. Jon L. Boyes
Vice Admiral, USN (Ret.)
AFCEA International President

JLB:pag
Enclosure

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0

include control, management and restoral of those critical NEMS components.

As we move further into the world of distributed systems and networks, the capability to control centrally our FEMA NEMS network will enhance our ability to respond quickly and effectively to national, regional, state or local emergencies.

• • • — • —

Protecting Our Secrets: Renewing the Commitment

William J. Casey
Director
Central Intelligence Agency

TODAY, intelligence is a commodity much in demand. Those who formulate national policy have come to depend upon timely, accurate intelligence. Besides the Central Intelligence Agency, the National Security Agency and the Defense Intelligence Agency, the Intelligence Community now includes elements of the Departments of State, Justice, Treasury, Defense, Energy and the military services. Likewise, the consumer community has expanded, extending well beyond the Executive Office of the President to congressional committees, their staffs, thousands of other government employees and thousands of contractors with a need-to-know because they build or operate collection systems or analyze the products of these systems.

While it is gratifying to realize that intelligence plays a vital role to so many, the large and expanding producer and consumer networks pose another problem—the effective safeguarding of our secrets. An intelligence service without secrets is a contradiction; moreover, it is not enough that intelligence activities and information be secret, they must remain secret.

Leaks hurt. They weaken the credibility of the U.S. government. They have cost us important sources, both human and technical, and they have created a psychological climate that chips away at intelligence capabilities and strains important relationships.

The increasing exposure of intelligence secrets in the media is a matter of great concern. All of us involved in the consumer and producer intelligence community must do a better job to protect classified information. Those of us who are cleared to receive classified intelligence are the first line of defense and must set the example. If we do not protect national security, who will?

It will always be a challenge (unique to a democracy) to maintain an effective intelligence service in an open society. But our future prosperity, quality of life and security demand that this service be nothing less than the best, including the most secure. Let us all rededicate ourselves to this task.

• • • — • —

VISTA

James C. Cercy
Brigadier General, USA
Commanding General
U.S. Army Electronics Research and Development Command

THE 1981 Army Science Board Summer Study resulted in recommendations that the Army strive to exploit those technologies in which the United States has a distinct development edge and that offer potentially high payback in terms of combat multipliers. In response to these recommendations, the Army identified five broad technological areas on which to focus management and funding resources with the ultimate goal of significantly increasing the operational effectiveness of U.S. forces. Very Intelligent Surveillance and Target Acquisition (VISTA) is one of these technology areas. The others are Distributed Command, Control, Communications and Intelligence (DC³I), Self Contained Munitions (SCM), Soldier Machine Interface (SMI) and Biotechnology (BIOTECH).

The primary purpose of the VISTA program is to demonstrate solutions to Mission Area Analysis deficiencies as related to battlefield data collection, data processing and combat information dissemination at the brigade level of operations.

VISTA is a graphics based approach that will allow the commander to see the battlefield, not just read it. Onboard sensor signal processing, as well as detailed interface definition, will permit the interconnectivity of sensors, processors and communications networks. VISTA will address the netting and integration of sensor data for subsequent near real time horizontal integration across the brigade's functional areas of maneuver control, fire support and intelligence/electronic warfare.

The VISTA program provides the user with the opportunity early in the development cycle to experience the operational benefits to be gained through the evaluation of advanced technology inserted into field exercise scenarios. VISTA, as well as all other technology integration efforts, relies heavily on the idea of

Sanitized Copy Approved for Release 2011/05/04 : CIA-RDP88G00186R000100100004-0